CLAIMS

What is claimed is:

1. A security system for a computer apparatus, wherein said computer apparatus includes a processor and system memory, said security system comprising:

at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities;

at least one utility module which under the direction from the processor, performs various utility functions with regards to the computer apparatus in response to the identified vulnerabilities; and

a security system memory which contains security information for performing the analysis of the computer apparatus.

2. The security system of claim 1 further including at least one graphical user interface in connection with the computer apparatus through which a system user may direct operations of the security system.

3. The security system of claim 2 further including a reporting module which provides status information to the GUI with regards to operations of the security system.

4. The security system of claim 1 wherein the security modules include at least one of:

a configuration/system module which performs an initial analysis of the computer system acquire configuration information;

a directory checking module which analyzes directories and files in the system memory to determine if security critical files have been tampered with;

a user manager module which analyzes the system memory with regards to improper of invalid permissions given to users of the system for accessing particular files;

an integrity checking module which analyzes files in the system memory to identify system vulnerabilities;

a network checking module which analyzes the computer apparatus to identify vulnerabilities created as a result of the computer apparatus connecting with a data network;

a password checking module which analyzes passwords for users of the computer apparatus to identify vulnerabilities.

5. The security system of claim 4 wherein the utilities modules include at least one of:

said user manager module which includes functionality to perform at least one of: create a user account, modify the user account, delete the user account, create a user template, edit the user template, and delete the user template;

a file removal module which deletes selected files from the system memory and removes links to the deleted file;

a file marking module which marks selected files; and

a scheduling module which may be employed to schedule any and all of the security modules to perform analysis of the system memory.

6. The security system of claim 2 wherein the computer apparatus comprises a Unix server.

7. The security system of claim 6 wherein the server is connected to a data network.

8. The security system of claim 2 wherein a plurality of interface screens are presented at the GUI for controlling operations of the security system.

9. The security system of claim 4 wherein the system memory comprises a list of known vulnerabilities which may be employed by the integrity checking module.

10. The security system of claim 4 wherein the system memory comprises dictionaries and other tools employed by the password checking module.

11. A method of providing a security assessment for a computer system which includes a system memory, comprising the steps of:

providing a security subsystem in the computer system such that functionality of the security subsystem is directed through a processor for the computer system, wherein the security performs steps comprising:

identifying a configuration of system;

accessing the system memory and performing at least one procedure to provide a security assessment for at least one aspect of the computer system;

as a result of any vulnerabilities discovered in the assessment, identifying corrective measures to be taken with regards to the computer system;

reporting the discovered vulnerability and the identified corrective measures; and

upon receiving an appropriate command, initiating the corrective measures.

12. The method of claim 11 wherein the step of performing at least one procedure to provide a security assessment includes at least one of:

performing an analysis of the directories and files in the system memory to determine if security critical files have been tampered with;

analyzing the system memory with regards to improper or invalid permission given to users of the system for accessing particular files;

analyzing the system memory to identify system vulnerabilities;

analyzing the computer apparatus to identify vulnerabilities created as a result of the computer apparatus connecting to a data network; and

analyzing passwords for users of the computer apparatus to identify vulnerabilities.

13. The method of claim 12 wherein based on the identified vulnerabilities at least one of the following steps are performed:

amending, deleting, or creating user accounts;

amending, deleting, or creating user templates;

deleting selected files from the system memory and removing links to said file;

marking of selected files within the system memory.

14. The method of claim 12 wherein the method of analyzing directories and files comprises the steps of:

accessing individual files in the system memory;

identifying the type of file contained therein;

making a determination as to whether the permissions for the identified file are secure;

if the permissions are not secure, providing a report describing the insecurity;

providing corrections for the detected files which are insecure and initializing corrective action upon receiving direction.

15. The method of claim 12 wherein the step of analyzing the system memory with regards to improper or invalid permissions given to users further comprises the steps of:

performing a check to see if a user owns his or her home directory;

performing a check to see if the user's group owns the home directory;

performing a check to see if user related files are valid; and

performing a check to see if the user's directory exists.

16. The method of claim 12 wherein the step of analyzing files in the system memory to identify system vulnerabilities further comprises the steps of:

providing a vulnerability database which includes a number of identified system vulnerabilities;

accessing the individual files in the system memory;

determining whether the file's owner matches a predetermined profile;

determining whether the file's group matches a predetermined profile;

determining whether the permissions associated with the file match a predetermined profile; and

determining whether the files predate a patch; and

providing a report on any vulnerabilities which may exist in the system memory.

17. The method of claim 12 wherein the step of analyzing the computer apparatus to identify vulnerabilities traded as a

result of the computer apparatus connecting with the data network: further comprises the steps of:

checking for insecure configuration files;

checking running of excessive system services; and

checking whether the computer system is running in the promiscuous mode.

18. The method of claim 12 wherein the step of analyzing passwords further comprises the step of:

identifying all passwords for the users of the computer system;

reading the passwords and for each identifying a next similar salt entry;

identifying a next predetermined number of words from the dictionary;

performing a word filtering method with regards to the passwords to add to the word list;

determining whether the word is in the list. If the word is in the list removing the user from the list.

19. The method of claim 11 further comprising the step of displaying result of the security analysis via a graphical user interface.

20. The method of claim 11 wherein the computer system is connected to a data network.